ABSTRACT

The invention relates to a method for enciphering a series of input symbols (5, 20) under application of a function (2), such as a substitution box and as a function of a series of key symbols (4). In order to reinforce the enciphering method in applications in which there is always used the same series of key symbols, there is provided a modification algorithm (9) with which, prior to enciphering, the function (8) is modified using symbols from the series of input symbols.

FIG. 2